

INDEX DIVISIBILITY IN DYNAMICAL SEQUENCES AND CYCLIC ORBITS MODULO p

ANNIE S. CHEN, T. ALDEN GASSERT, AND KATHERINE E. STANGE

ABSTRACT. Let $\phi(x) = x^d + c$ be an integral polynomial of degree at least 2, and consider the sequence $(\phi^n(0))_{n=0}^\infty$, which is the orbit of 0 under iteration by ϕ . Let $D_{d,c}$ denote the set of positive integers n for which $n \mid \phi^n(0)$. We give a characterization of $D_{d,c}$ in terms of a directed graph and describe a number of its properties, including its cardinality and the primes contained therein. In particular, we study the question of which primes p have the property that the orbit of 0 is a single p -cycle modulo p . We show that the set of such primes is finite when d is even, and conjecture that it is infinite when d is odd.

1. INTRODUCTION

A dynamical sequence is the orbit $\alpha, \phi(\alpha), \phi^2(\alpha), \dots$ of some α in a ring R under iteration of a map $\phi : R \rightarrow R$. In arithmetic dynamics, one takes ϕ to be a rational map defined over a number field and α to be an algebraic number. Such dynamical sequences have many properties in common with their more well-known cousins: recurrence sequences and algebraic divisibility sequences arising from algebraic groups, such as Lucas sequences and elliptic divisibility sequences. In particular, all such sequences a_n are *divisibility sequences*, i.e. whenever $n \mid m$, then $a_n \mid a_m$.

The study of the primes appearing in such sequences has a centuries-long history dating back at least to Fermat's study of primes of the form $2^{2^n} + 1$. The primes appearing in a dynamical sequence encode information about the dynamical system in residue fields. For example, taking $R = \mathbb{Z}$, if $p \mid \phi^n(0)$, then 0 has period dividing n in the dynamical system $\phi : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$. In

Date: August 9, 2016.

2010 *Mathematics Subject Classification.* Primary: 37P05, 37P25, 11Y55, Secondary: 11B37, 11B39, 11B50, 11G99.

Key words and phrases. arithmetic dynamics, dynamical portrait, index divisibility, cycle, orbit, functional digraph, dynamical sequence, polynomial map, iteration, quadratic map, divisibility sequence, integer sequence, post-critical orbit.

The third author's work was supported by the National Security Agency grant H98230-16-1-0040 and National Science Foundation grant DMS-1643552.

particular, $p \mid \phi^p(0)$ if and only if the dynamical system given by ϕ on $\mathbb{Z}/p\mathbb{Z}$ consists of a single orbit of size 1 or p . Silverman studied the statistics of orbit sizes for rational maps modulo a varying prime p [22] (see also [8]).

In this paper, we restrict ourselves to the study of the maps $\phi(x) = x^d + c \in \mathbb{Z}[x]$, where $d \geq 2$. The orbit structure for $x^2 + c$ is of particular interest for primality testing, integer factorization and pseudo-random number generation [6, 17, 19]. Silverman collected some numerical data on quadratic maps $x^2 + c$ [22], while Peinado, Montoya, Muñoz and Yuste give explicit upper bounds for the cycle sizes of $x^2 + c$ in a finite field [18]; more explicit structure is known for the exceptional maps x^2 and $x^2 - 2$ [28]. Jones [15] found that the natural density of primes dividing at least one nonzero term of a dynamical sequence is zero for four infinite families of quadratic functions, including $\phi(x) = x^2 + c$, where $c \in \mathbb{Z}$ and $c \neq 1$. Hamblen, Jones, and Madhu [11] later generalized the results to $\phi(x) = x^d + c$ (see also [5]). In other words, the primes p for which 0 is periodic (instead of pre-periodic) are of density zero. These results imply that the primes p for which the dynamical system consists of a single p -cycle modulo p are of density zero.

Let $S_{d,c}$ be the set of primes p such that the dynamical system $\phi : \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ consists of a single p -cycle. We show the following.

Theorem 1.1. *Let $\phi(x) = x^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$. Then whenever d is even and c is odd, $S_{d,c} = \{2\}$; while if d is even and c is even, then $S_{d,c} = \emptyset$.*

Based on numerical data and heuristics, we conjecture that there are infinitely many such primes otherwise.

Conjecture 1.2. $S_{d,c}$ is infinite whenever d is odd.

Using an analysis of the cycle structure of the permutation $x \mapsto x^d$ on $\mathbb{Z}/p\mathbb{Z}$, we are able to somewhat restrict the set $S_{d,c}$ as follows.

Theorem 1.3. *If $d \equiv 3 \pmod{4}$, and $p \equiv 1 \pmod{4}$ is prime, then $p \notin S_{d,c}$.*

For example, when d is an odd power of 3, we conclude that $S_{d,c}$ contains only primes congruent to 11 (mod 12) (Corollary 4.4).

Theorem 1.1 is a consequence of our study of *index divisibility* in dynamical sequences. The question of index divisibility for a sequence $(a_n)_0^\infty$ seeks to characterize those integers $n \geq 1$ such that $n \mid a_n$. It has a substantial history for Fibonacci and Lucas sequences [3, 12, 14, 25, 26, 27, 29], and has also been studied for elliptic divisibility sequences [10, 24] and general linear recurrences [2]. As another example, composite integers n for which $n \mid a^n - a$ are called pseudoprimes to the base a .

Throughout, let $\phi(x) = x^d + c \in \mathbb{Z}[x]$ where $d \geq 2$, let (W_n) denote the orbit of 0 under ϕ , i.e. $W_n = \phi^n(0)$, and define

$$D_{d,c} := \{n \in \mathbb{Z} : n \geq 1, n \mid W_n\}, \quad \text{and} \quad P_{d,c} := \{p \in D_{d,c} : p \text{ is prime}\}.$$

In the spirit of Smyth and of Silverman and Stange [24, 25], we represent $D_{d,c}$ by a directed graph that connects each element to its minimal multiples. To construct this *index divisibility graph* G , initially let 1 be in the vertex set G_V , then add vertices and edges to G iteratively according to the the following rules.

Let $v_p(x)$ denote the p -adic valuation of an integer x . For each $n \in G_V$, adjoin the vertex pn and the directed edge (n, np) if

- (1) p is a prime satisfying $v_p(\phi^n(0)) > v_p(n)$ (edge of *type 1*), or
- (2) $p \in P_{d,c}$ satisfies $v_p(n) = 0$ (edge of *type 2*).

Our main results provide a characterization of $D_{d,c}$ and $P_{d,c}$ in terms of this graph.

Theorem 1.4. *Let $\phi(x) = x^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$. Let G be the index divisibility graph corresponding to ϕ , and let G_V be the vertex set of G . Then $G_V = D_{d,c}$.*

Theorem 1.5. *Let $\phi(x) = x^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$. Then $P_{d,c}$ satisfies the following.*

- (1) $2 \in P_{d,c}$.
- (2) *Every divisor of c is an element of $D_{d,c}$. In particular, if p is prime and $p \mid c$, then $p \in P_{d,c}$.*
- (3) *If p is prime and $d \equiv 1 \pmod{p-1}$, then $p \in P_{d,c}$.*

If d is even, then we are able to fully characterize $P_{d,c}$.

Theorem 1.6. *If d is even, then*

$$P_{d,c} = \{2\} \cup \{p \text{ prime} : p \mid c\}.$$

Theorem 1.1 is an immediate consequence.

Two main tools we use in our investigation are the notions of a *rigid divisibility sequence* and of a *primitive prime divisor*.

An integer sequence (a_n) is a *rigid divisibility sequence* if for every prime p the following two properties hold:

- (1) if $v_p(a_n) > 0$, then $v_p(a_{nk}) = v_p(a_n)$ for all $k \geq 1$, and

(2) if $v_p(a_n) > 0$ and $v_p(a_m) > 0$, then $v_p(a_n) = v_p(a_m) = v_p(a_{\gcd(m,n)})$.

In particular, rigid divisibility sequences are divisibility sequences.

Rice [20] showed that for any polynomial $\phi \in \mathbb{Z}[x]$ of degree $d \geq 2$ where 0 is a wandering point (i.e. of infinite orbit), the integer sequence $(\phi^n(0))$ is a rigid divisibility sequence if and only if the coefficient of the linear term of ϕ is zero. In particular, this means that the orbit of zero under $\phi(x) = x^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$, is a rigid divisibility sequence.

Given a sequence (a_n) of integers, the term a_n contains a *primitive prime divisor* if there exists a prime p such that $p \mid a_n$, but $p \nmid a_i$ for all $0 < i < n$. The study of primitive prime divisors dates back to Bang and Zsigmondy, who showed that every term of the sequence $(a^n - b^n)$, where $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, has a primitive prime divisor [4, 30]. Carmichael's Theorem asserts that the same is true for the Fibonacci numbers beyond the 12th term [7]. The *Zsigmondy set* is the set of terms not having a primitive prime divisor; for the Fibonacci numbers, it is $\{1, 2, 6, 12\}$. Similarly, Silverman has shown that elliptic divisibility sequences have finite Zsigmondy sets [23].

Turning to dynamical sequences, Rice [20] showed that if $\phi(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree $d \geq 2$, and $(\phi^n(0))$ is an unbounded rigid divisibility sequence, then all but finitely many terms contain a primitive prime divisor. Ingram and Silverman [13] generalized the results to rational functions over number fields. Doerksen and Haensch [9] extended upon this by finding explicit upper bounds on the Zsigmondy set for certain polynomial maps.

The following examples illustrate our results.

Example 1.7. Suppose $\phi(x) = x^2 + 3$. Then the orbit of 0 is

$$0, 3, 12, 147, 21612, 467078547, \dots$$

Here,

$$D_{2,3} = \{1, 2, 3, 4, 6, 12, 21, 42, \dots\} \quad \text{and} \quad P_{2,3} = \{2, 3\}$$

by Theorems 1.5 and 1.6. The index divisibility graph is shown in Figure 1.

Notice in Figure 1 that all type 2 edges are also type 1 edges. However, this is not always the case, as shown in Figure 2.

Example 1.8. Suppose $\phi(x) = x^3 + 4$. Then the orbit of 0 is:

$$0, 4, 68, 314436, \dots$$

The index divisibility graph is illustrated in Figure 2.

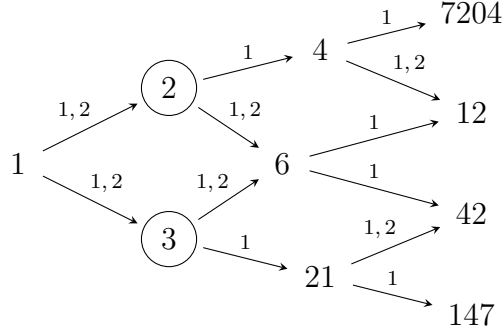


FIGURE 1. A portion of the index divisibility graph for $\phi(x) = x^2 + 3$. The circled vertices are elements of $P_{2,3}$, and edges are labeled by their type.

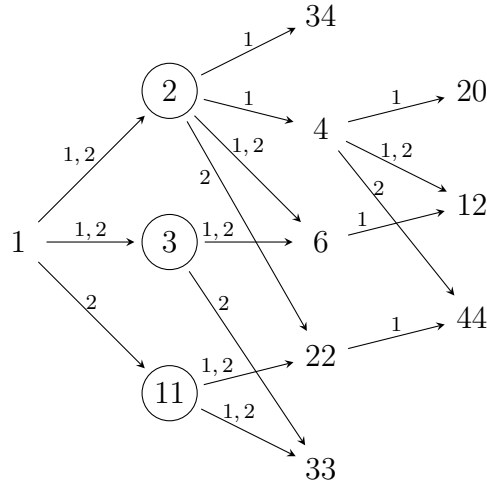


FIGURE 2. A portion of the index divisibility graph for $\phi(x) = x^3 + 4$. The circled vertices are elements of $P_{3,4}$, and edges are labeled by their type.

In Section 2, we study index divisibility and prove Theorems 1.1, 1.4, 1.5, and 1.6.

In Section 3, we classify the finiteness of $D_{d,c}$: it is finite exactly when $(d, c) = (2, 1)$, $(2, -2)$, or $(d, 1)$ where $d \geq 4$ is even (see Theorem 3.3).

In Section 4, we study $P_{d,c}$ and its subset $S_{d,c}$ in the case where d is odd, and prove Theorem 1.3.

In Section 5, as a computational experiment, we find all pairs (p, c) , where $0 < c < p/2$ and $p \leq 37619$, for which p is in $S_{3,c}$ (see Figure 3). We provide some heuristics to support Conjecture 1.2.

Finally, in Section 6, we ask the question, for a fixed n , of which pairs (d, c) satisfy $n \in D_{d,c}$.

Acknowledgements. The authors would like to thank the Boulder Valley School District's Science Research Seminar program for making this research project possible, and would like to thank the first author's teacher in that program, Ryan O'Block, for his support.

2. INDEX DIVISIBILITY

For the remainder of the paper, we maintain the notation presented in the introduction, namely $\phi(x) = x^d + c$ is an integral polynomial of degree at least 2, $W_n = \phi^n(0)$, $D_{d,c} = \{n \in \mathbb{Z} : n \geq 1, n \mid W_n\}$, and $P_{d,c}$ is the set of primes in $D_{d,c}$.

Before proceeding to the proofs, we identify two significant properties of $D_{d,c}$.

Lemma 2.1. *Suppose $n \in D_{d,c}$ and let p be the smallest prime divisor of n . Then $p \in D_{d,c}$.*

Proof. Let $n \in D_{d,c}$, and write $n = pm$, where p is the smallest prime factor of n . Then $p \mid W_n$ as $p \mid n$ and $n \mid W_n$. In particular, 0 is periodic modulo p , so letting b denote the period of 0, it follows that $0 < b \leq p$, $p \mid W_b$, and $b \mid n$. However, since p is the smallest factor of n greater than 1, either $b = 1$ or $b = p$. If $b = p$, then $p \mid W_p$ as desired. Otherwise, if $b = 1$, then $p \mid W_1$, and hence $p \mid W_p$ since $W_1 \mid W_p$. \square

Lemma 2.2. *If $a, b \in D_{d,c}$ are relatively prime, then $ab \in D_{d,c}$.*

Proof. Let a and b be relatively prime numbers in $D_{d,c}$. Since (W_n) is a rigid divisibility sequence, we have that $a \mid ab$ implies $W_a \mid W_{ab}$, and $b \mid ab$ implies $W_b \mid W_{ab}$. Then because $a \mid W_a$, $a \mid W_{ab}$. Similarly, because $b \mid W_b$, we have $b \mid W_{ab}$. Since a and b are relatively prime, $ab \mid W_{ab}$, and so $ab \in D_{d,c}$. \square

We now proceed to prove Theorem 1.4.

Proof of 1.4. First we show $G_V \subseteq D_{d,c}$. To begin, we have $1 \mid W_1$, and so $1 \in D_{d,c}$.

Next we show that if $n \in D_{d,c}$ and $(n, np) \in G_E$ (the edge set of G), then $pn \in D_{d,c}$. We examine edges of type 1. Suppose there exist $n \in D_{d,c}$ and a prime p such that $v_p(W_n) > v_p(n)$. Since $n \mid W_n$ and $v_p(W_n) > v_p(n)$, we see that $np \mid W_n$. Then since (W_n) is a rigid divisibility sequence, $n \mid np$ implies $W_n \mid W_{np}$. Thus $np \mid W_{np}$, and so $np \in D_{d,c}$.

For edges of type 2, if $p \in P_{d,c}$ and $p \nmid n$, then $np \in D_{d,c}$ by Lemma 2.2. Thus we have shown that $G_V \subseteq D_{d,c}$.

We now proceed to show $D_{d,c} \subseteq G_V$. Suppose $n \in D_{d,c}$. To prove that $n \in G_V$, we show that G contains a path from 1 to n . If $n = 1$, there is nothing to show, so let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factorization of n , where $p_1 < p_2 < p_3 < \cdots < p_k$. From Lemma 2.1, we know that $p_1 \in D_{d,c}$, hence $(1, p_1)$ is an edge of type 2 in G .

Now suppose $1 \leq i \leq k$ and m is the largest divisor of n supported on primes p_j , where $j < i$. Then we have two observations:

- (1) If $p_i \in P_{d,c}$, then (m, mp_i) is an edge of type 2. If $p_i \notin P_{d,c}$, then 0 has order less than p_i modulo p_i , which implies $p_i \mid W_m$. Then $v_{p_i}(W_m) > v_{p_i}(m)$, and so (m, mp_i) is an edge of type 1.
- (2) Suppose $1 \leq t < \alpha_i$. Furthermore, $p_i \mid W_{mp_i^t} \mid W_{mp_i^{t+1}}$ (otherwise, the order of 0 modulo p_i exceeds p_i). By rigid divisibility, $v_{p_i}(W_{mp_i^t}) = v_{p_i}(W_n) \geq \alpha_i > t = v_{p_i}(mp_i^t)$. Therefore, we also have an edge of type 1: (mp_i^t, mp_i^{t+1}) .

Combining these observations, starting with 1, we have the following path of directed edges from 1 to n :

$$\begin{aligned}
 1 &\xrightarrow{2} p_1 \xrightarrow{1} p_1^2 \xrightarrow{1} \cdots \xrightarrow{1} p_1^{\alpha_1} \\
 &\xrightarrow{1 \text{ or } 2} p_1^{\alpha_1} p_2 \xrightarrow{1} p_1^{\alpha_1} p_2^2 \xrightarrow{1} \cdots \xrightarrow{1} p_1^{\alpha_1} p_2^{\alpha_2} \\
 &\xrightarrow{1 \text{ or } 2} \cdots \\
 &\xrightarrow{1 \text{ or } 2} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k \xrightarrow{1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^2 \xrightarrow{1} \cdots \xrightarrow{1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = n.
 \end{aligned}$$

Thus, $D_{d,c} \subseteq G_V$. □

We next prove Theorem 1.5.

Proof of 1.5. First, $W_2 = c^d + c = c^{d-1}(c+1)$. It follows that $2 \mid W_2$, and thus $2 \in P_{d,c}$.

Next, to prove that every prime divisor of c is an element of $D_{d,c}$, it suffices to show that $c \mid W_n$ for all n , for then it follows that every divisor of c is

an element of $D_{d,c}$. We proceed via induction on n . When $n = 0$, we have $W_n = W_0 = 0$, hence $c \mid W_0$. Next assume the statement holds for $n = k$. Then $W_{k+1} = (W_k)^d + c$. Now since $c \mid W_k$, we have $c \mid (W_k)^d$, and so $c \mid W_{k+1}$.

For the third property, we show that if p is prime, then $p \in P_{d,c}$ if $d \equiv 1 \pmod{p-1}$. Let $d = (p-1)k + 1$, where $k \in \mathbb{Z}$. We have $\phi(x) = x^d + c = x^{(p-1)k+1} + c \equiv x + c \pmod{p}$, so $\phi^p(x) \equiv x + pc \equiv x \pmod{p}$. In particular, this means that $W_p = \phi^p(0) \equiv 0 \pmod{p}$, so $p \in P_{d,c}$. \square

We now prove Theorem 1.6.

Proof of 1.6. Let d be even. We show that if p is an odd prime, then $p \in P_{d,c}$ only if $p \mid c$.

Suppose that $p \in P_{d,c}$. Then $p \mid W_p$, and the period of 0 modulo p is a divisor of p . If the period of 0 is 1, then $p \mid W_1 = c$. Otherwise if the period of 0 is p , then 0 has a unique preimage modulo p . In particular, $\sqrt[d]{-c} \equiv -\sqrt[d]{-c} \pmod{p}$. Therefore $\sqrt[d]{-c} \equiv 0 \pmod{p}$, so $c \equiv 0 \pmod{p}$. \square

In conjunction with Theorem 1.5, Theorem 1.6 provides a full characterization for $P_{d,c}$ when d is even. In particular, we can now prove Theorem 1.1.

Proof of 1.1. When c is odd, the orbit of 0 has period 2. When c is even, the orbit of 0 has period 1. When $p \mid c$, the orbit of 0 has period 1. \square

3. CARDINALITY OF $D_{d,c}$

In Theorem 3.3, we identify all pairs (d, c) for which $D_{d,c}$ is finite. But first, we note some simple infinite cases where $D_{d,c}$ is explicit.

Lemma 3.1.

- (1) For all d , $D_{d,0}$ is the set of positive integers.
- (2) If d is even, then $D_{d,-1}$ is the set of even positive integers.

Proof. If $c = 0$, then $W_n = 0$ for all n . When $c = -1$, then

$$W_n = \begin{cases} 0 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd.} \end{cases}$$

In both cases, the result is immediate. \square

We now provide a simple yet sufficient condition for $D_{d,c}$ to be infinite.

Lemma 3.2. *If there exists $n \in D_{d,c}$ such that $n \geq 3$, then $D_{d,c}$ is infinite.*

Proof. Suppose that $n \in D_{d,c}$ for some $n \geq 3$. From [9], W_n contains a primitive prime divisor p , and since p is primitive, we have $n \leq p$. Since p appears as a divisor in the sequence, 0 is periodic modulo p , and the period cannot exceed p . Hence either $p = n$, or p and n are coprime. If the latter holds, then, by Theorem 1.4, there is an edge of type 2: (n, np) . This implies that n is not the largest element of $D_{d,c}$. Therefore it suffices to consider the case $p = n$.

First, suppose that d is even and $p = n$. Then, by Theorem 1.6, we have $p \mid c$, so that $p \mid W_n$ for all n . This contradicts primitivity, so d must be odd.

Therefore, suppose that d is odd and $p = n$. In this case, write $W_p = pm$ for some integer m . If $|m| > 1$, then for each prime divisor q of m , the index divisibility graph contains the edge (p, pq) , hence p is not the largest element of $D_{d,c}$.

Thus we are left considering the case d is odd, $p = n$, and $W_p \in \{0, \pm p\}$. However, we claim that this is not possible, by the growth of W_n . For, since d is odd, the signs of W_n , W_n^d , and c are all the same by induction. This implies that $|W_{n+1}| = |W_n^d + c| = |W_n^d| + |c| \geq |W_n|^d$. In particular, since $|W_2| \geq 2$, we have $|W_n| > 2^{d^{n-2}}$. (Here we use that $|c| \geq 1$. The case $c = 0$ is covered by Lemma 3.1.) This rules out $|W_p| \leq p$ for any $p \geq 3$. \square

Consequently, $D_{d,c}$ is infinite in most cases.

Theorem 3.3. *The set $D_{d,c}$ is finite if and only if either*

- (1) d is even and $c = 1$, or
- (2) $d = 2$ and $c = -2$.

Moreover, if $D_{d,c}$ is finite, then $D_{d,c} = \{1, 2\}$.

Proof. By Theorem 1.5, $c \in D_{d,c}$, hence it follows from Lemma 3.2 that $D_{d,c}$ is infinite whenever $|c| \geq 3$. Similarly, if d is odd, then $3 \in P_{d,c}$ by Theorem 1.5, and again $D_{d,c}$ is infinite.

For the remainder of the proof, assume that d is even. The cases $c = 0$ and $c = -1$ are handled by Lemma 3.1, leaving only the cases $c = 1$ and $c = -2$ to consider.

Suppose $c = 1$. In this case $W_1 = 1$ and $W_2 = 2$, and by Theorem 1.6, we have $P_{d,1} = \{2\}$. Following the construction of the index divisibility graph, we have a single edge of type 2 emanating from the vertex 1 (the edge $(1, 2)$), and there are no edges emanating from the vertex 2. Thus $D_{d,1} = \{1, 2\}$.

Suppose $c = -2$. If $d = 2$, then $W_1 = -2$ and $W_2 = 2$. Similar to the previous case, the index divisibility graph only contains a single edge—the edge $(1, 2)$ —and hence $D_{2,-2} = \{1, 2\}$.

Otherwise suppose $d \geq 4$. Then $W_2 = (-2)^d - 2 = -2((-2)^{d-1} + 1)$, where $|(-2)^{d-1} + 1| > 1$ and is odd. Hence W_2 has an odd prime divisor p , and therefore $(2, 2p)$ is an edge of type 1 in the index divisibility graph. Since $2p \in D_{d,-2}$, it follows that $D_{d,-2}$ is infinite. \square

4. $S_{d,c}$ AND p -CYCLES MODULO p

In Theorem 1.5, we give a description of the set $P_{d,c}$. In the case that d is even, Theorem 1.6 concludes that Theorem 1.5 completely determines $P_{d,c}$. However, when d is odd, the conditions in Theorem 1.5 are insufficient to completely describe the set. This insufficiency is illustrated in Example 1.8 where we see that $11 \in P_{3,4}$, yet 11 does not satisfy any of the conditions in Theorem 1.5.

Suppose then that $p \in P_{d,c}$ where both p and d are odd. As we have previously noted, if $p \in P_{d,c}$, then the period of 0 in $\mathbb{Z}/p\mathbb{Z}$ is a divisor of p . If that period is 1, then $p \mid c$, which Theorem 1.5 already accounts for. Therefore, the primes that are the exception are the odd primes for which 0 has period p modulo p . In other words, the primes of interest are the odd primes p for which $x^d + c$ induces a single cycle of size p in $\mathbb{Z}/p\mathbb{Z}$.

It is well known that $\pi(x) = x^d$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$ if and only if $\gcd(d, p-1) = 1$. Hence under the same conditions, it follows that $x^d + c$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$. In particular, we have $\phi = \tau^c \circ \pi$ (over $\mathbb{Z}/p\mathbb{Z}$), where $\tau(x) = x + 1$. Since every p -cycle is an even permutation, we see that ϕ is a p -cycle only if π is an even permutation. Equivalently, if π is an odd permutation of $\mathbb{Z}/p\mathbb{Z}$, then $p \notin P_{d,c}$.

We now use this observation to prove Theorem 1.3. For the remainder of this section, let $\text{ord}_n m$ denote the order of m in $(\mathbb{Z}/n\mathbb{Z})^*$.

In order to understand the sign of π as a permutation, we consider its cycle structure, which is given thusly.

Lemma 4.1. *Suppose $\pi(x) = x^d$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$. Then π has a cycle of length m if and only if there exists a divisor k of $p-1$ such that $\text{ord}_k d = m$. Moreover, the number of cycles N_m of length m satisfies*

$$mN_m = \sum_{i|m, i < m} iN_i.$$

Proof. See Lidl and Mullen [16, Theorem 1], as well as Ahmad [1, Theorem 1] for a more general statement. \square

In particular, letting φ denote the Euler totient function, the theory of cyclic groups gives the following cycle structure.

Lemma 4.2. *Let p be prime, and suppose $\gcd(d, p-1) \neq 1$. Then $x \mapsto x^d$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$ with the following cycle structure:*

- (1) 0 is fixed, and
- (2) for each divisor k of $p-1$, there are $\varphi(k)$ elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of order $\text{ord}_k d$, i.e. the permutation contains $\varphi(k)/(\text{ord}_k d)$ cycles of length $\text{ord}_k d$ for each divisor k of $p-1$.

The following Lemma will also prove useful.

Lemma 4.3. *Let d be an odd integer, let $\mu = v_2(d-1)$, and let $\nu = v_2(d^2-1)-1$ (i.e. $\nu = \max\{v_2(d-1), v_2(d+1)\}$). Then*

$$\text{ord}_{2^k} d = \begin{cases} 1 & 0 \leq k \leq \mu \\ 2 & \mu < k \leq \nu \\ 2^{k-\nu} & \nu < k. \end{cases}$$

Proof. If $v_2(d-1) \geq k$, then $d \equiv 1 \pmod{2^k}$, hence $\text{ord}_{2^k} d = 1$. If $v_2(d+1) \geq k > 1$, then $d \equiv -1 \pmod{2^k}$, hence $\text{ord}_{2^k} d = 2$. Otherwise $v_2(d^{2^j}-1) = \nu + j$, and it follows that $2^{k-\nu}$ is the order of d . \square

Proof of Theorem 1.3. Let p be a prime where $p \equiv 1 \pmod{4}$. We will show that $\pi(x) = x^d$ is an odd permutation of $\mathbb{Z}/p\mathbb{Z}$ if and only if $d \equiv 3 \pmod{4}$, which by the discussion at the start of this section is sufficient to prove the theorem. Moreover, we assume that $\gcd(d, p-1) = 1$, as this is both necessary and sufficient for π to be a permutation.

The cycle type of π is given in Lemma 4.2. Let $N_k = \varphi(k)/(\text{ord}_k d)$ be the number of cycles of length k in π . Since a k -cycle is the product of $k-1$ transpositions, we see that π may be written as a product of the following number of transpositions:

$$\begin{aligned} \sum_{k|p-1} N_k((\text{ord}_k d) - 1) &= \sum_{k|p-1} \varphi(k) - \sum_{k|p-1} N_k \\ &= p-1 - \sum_{k|p-1} N_k. \end{aligned}$$

It now suffices to determine when $\sum_{k|p-1} N_k$ is odd.

To count the cycles, write $p-1 = 2^\lambda \omega$, where ω is odd. Then

$$\sum_{k|p-1} N_k = \sum_{\delta|\omega} \sum_{0 \leq i \leq \lambda} N_{2^i \delta}.$$

Consider first the sum over $\delta > 1$; we will show that this is even. Using the same notation as in Lemma 4.3, let $\mu = v_2(d-1)$ and $\nu = v_2(d^2-1) - 1$. Then for each δ , we have

$$\sum_{0 \leq i \leq \lambda} N_{2^i \delta} = N_\delta + N_{2\delta} + \sum_{2 \leq i \leq \mu} \frac{\varphi(2^i \delta)}{\text{ord}_{2^i \delta} d} + \sum_{\mu < i \leq \nu} \frac{\varphi(2^i \delta)}{\text{ord}_{2^i \delta} d} + \sum_{\nu < i \leq \lambda} \frac{\varphi(2^i \delta)}{\text{ord}_{2^i \delta} d}.$$

Note that $N_\delta + N_{2\delta} = 2N_\delta$ since

$$N_{2\delta} = \frac{\varphi(2\delta)}{\text{lcm}(\text{ord}_2 d, \text{ord}_\delta d)} = \frac{\varphi(\delta)}{\text{ord}_\delta d} = N_\delta.$$

Next, $\text{ord}_{2^i \delta} d = \text{lcm}(\text{ord}_{2^i} d, \text{ord}_\delta d)$ by the Chinese remainder theorem. Moreover, $\text{ord}_\delta d \mid \varphi(\delta)$ because $\varphi(\delta) = |(\mathbb{Z}/\delta\mathbb{Z})^*|$, and $\text{ord}_\delta d$ is the order of d in $(\mathbb{Z}/\delta\mathbb{Z})^*$. Hence

$$\sum_{2 \leq i \leq \mu} \frac{\varphi(2^i \delta)}{\text{ord}_{2^i \delta} d} = \sum_{2 \leq i \leq \mu} \frac{2^{i-1} \varphi(\delta)}{\text{ord}_\delta d} \equiv 0 \pmod{2},$$

Now since $i \geq 2$,

$$\sum_{\mu < i \leq \nu} \frac{\varphi(2^i \delta)}{\text{ord}_{2^i \delta} d} = \sum_{\mu < i \leq \nu} \frac{2^{i-1} \varphi(\delta)}{\text{lcm}(2, \text{ord}_\delta d)} \equiv 0 \pmod{2},$$

and similarly,

$$\sum_{\nu < i \leq \lambda} \frac{\varphi(2^i \delta)}{\text{ord}_{2^i \delta} d} = \sum_{\nu < i \leq \lambda} \frac{2^{i-1} \varphi(\delta)}{\text{lcm}(2^{k-v}, \text{ord}_\delta d)} \equiv 0 \pmod{2}.$$

We conclude that the portion of the sum where $\delta > 1$ is even.

We are left to consider the contribution from $\delta = 1$. Here,

$$\begin{aligned} \sum_{0 \leq i \leq \lambda} N_{2^i} &= \sum_{0 \leq i \leq \lambda} \frac{\varphi(2^i)}{\text{ord}_{2^i} d} \\ &= 2 + \sum_{2 \leq i \leq \lambda} \frac{2^{i-1}}{\text{ord}_{2^i} d} \\ &\equiv \begin{cases} 1 \pmod{2} & \text{if } v_2(d-1) = 1 \\ 0 \pmod{2} & \text{otherwise.} \end{cases} \end{aligned}$$

Therefore, π is odd if and only if $d \equiv 3 \pmod{4}$, concluding the proof. \square

Corollary 4.4. *If $p \in P_{3^k, c}$ and k is odd, then either $p = 2$, $p \mid c$, or $p \equiv 11 \pmod{12}$.*

Proof. The cases $p = 2$ and $p \mid c$ are due to Theorem 1.5. Otherwise, if $p \in P_{3^k, c}$, k is odd, and $p \nmid c$, then $x^{3^k} + c$ is a cyclic permutation of $\mathbb{Z}/p\mathbb{Z}$, and hence $p \not\equiv 1 \pmod{3}$. Finally, $p \not\equiv 5 \pmod{12}$ by Theorem 1.3. \square

As evidenced in Example 1.8, primes falling into this third category do exist.

5. HEURISTICS AND EXPERIMENT FOR $S_{d, c}$

In this section, we provide some data to support Conjecture 1.2 in the case that $d = 3$ and $d = 9$, and consider some heuristic arguments.

In Figure 3, we plot all pairs $(p, c) \in [3, 37619] \times [1, p/2]$ for which $p \in S_{3, c}$. When d is odd, if $p \in S_{d, c}$, then $p \in S_{d, c'}$ for any $c' \equiv \pm c \pmod{p}$ (Proposition 6.1); hence the restriction to the interval $[1, p/2]$. The data indicates that these pairs occur somewhat frequently and that the pairs $(p, c/p)$ seem to be distributed uniformly randomly in the rectangle $[1, 37619] \times [0, 0.5]$.

Based on this observation, as c is restricted to integral values in $[1, (p-1)/2]$, let us adopt the following heuristic assumption:

Hypothesis 5.1. *For any fixed c the probability that a prime $p \geq 2|c|$ satisfies $p \in S_{3, c}$ is $2/(p-1)$.*

Under this hypothesis, we may compute the expected number of pairs (p, c) in the data set for any given c . Namely, the expectation for the number of data points for any fixed c is

$$E_X(c) = \sum_{\substack{p \in [2|c|, X] \\ p \equiv 11 \pmod{12}}} \frac{2}{p-1}.$$

In particular, $E_X(c) \rightarrow \infty$ as $X \rightarrow \infty$. This quantity $E_X(c)$ is compared to the actual count for our data ($X = 37619$) in Figure 4.

In Figure 5, we see that for approximately 60% of $11 \pmod{12}$ primes, there exists a c for which $p \in P_{3, c}$. Similarly in Figure 6, for just under 50% of primes that are $5 \pmod{6}$, there exists a c such that $p \in P_{9, c}$. (Corollary 4.4 does not apply here; however we may restrict to $p \equiv 5 \pmod{6}$ since if $p \equiv 1 \pmod{6}$, then $\gcd(p-1, 9) > 1$, so $x^9 + c$ is not a permutation of $\mathbb{Z}/p\mathbb{Z}$.) Of these primes, approximately two-thirds of them are $11 \pmod{12}$.

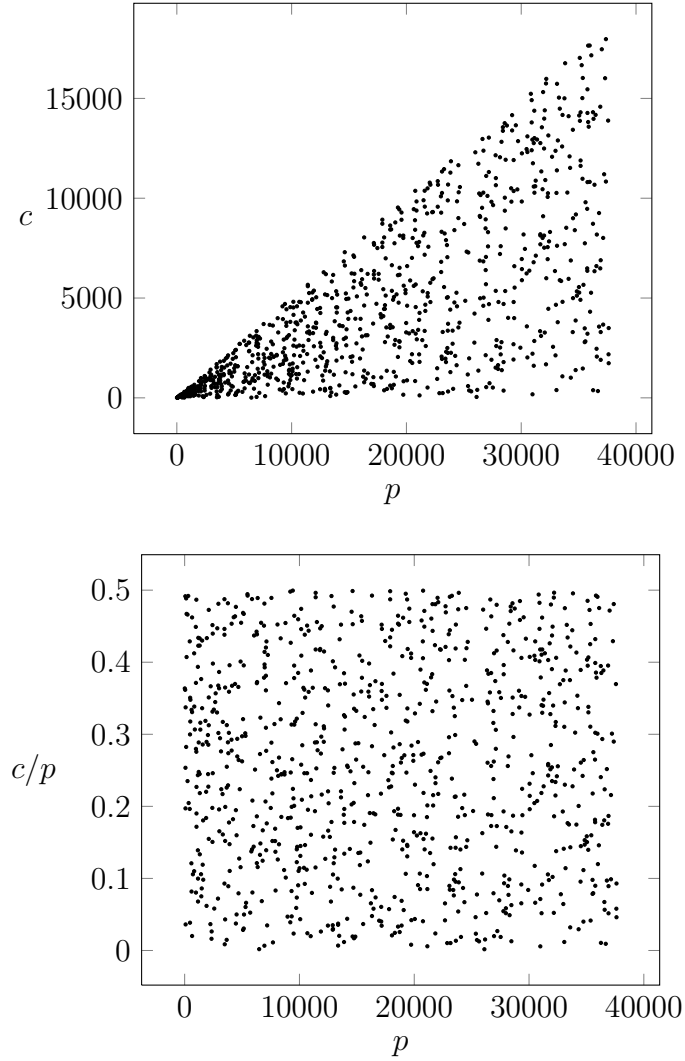


FIGURE 3. The graph on the top shows a scatterplot of pairs (p, c) such that $p \leq 37619$ is prime and $p \in S_{3,c}$. Below, the same scatterplot is scaled so that the pairs are of the form $(p, c/p)$.

We finish this section with a brief discussion of the relationship to dynatomic polynomials. That is, fixing p , the number of $1 \leq c \leq p-1$ for which $p \in S_{3,c}$ is the number of non-zero roots of a dynatomic polynomial, as follows. Given a family of maps ϕ_c (for us, $\phi_c(x) = x^3 + c$), write $\Psi_{n,0}(c) \in \mathbb{Z}[c]$ for the

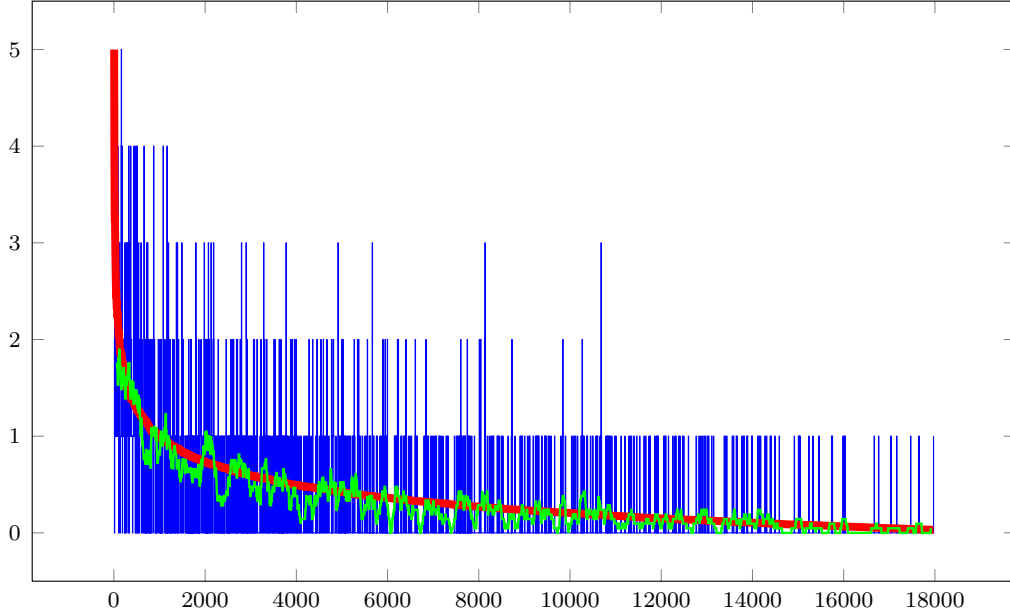


FIGURE 4. The data in Figure 3 is collected in this figure by c value in bins of size 6. For each $k \in \mathbb{N}$, the value of the blue graph on the interval $[6(k-1), 6k)$ is the number of pairs (p, c) in the data for which $6(k-1) \leq c < 6k$. At each point x , the green line is the average of the blue function over the interval $(x-60, x+60)$. The red line is the theoretical expectation under the assumption that the data is random, i.e. it is the graph of $E_{37619}(x)$.

polynomial whose roots are those c for which 0 has period n , i.e.

$$\Psi_{n,0}(c) = \phi_c^n(0).$$

Then the n -th dynatomic polynomial $\Phi_{n,0}(c)$ is defined so that

$$\Psi_{n,0} = \prod_{d|n} \Phi_{d,0}.$$

In particular, $\Phi_{n,0}$ has as roots those c such that 0 has minimal period n under the map $x^3 + c$. For more on these standard definitions, see [21].

With this setup, for a fixed p , the number of $1 \leq c \leq p-1$ for which $p \in S_{3,c}$ is equal to the number of non-zero roots of $\Phi_{p,0}(c)$ modulo p . One should note that the cyclotomic polynomials, which are considered analogous to the dynatomic polynomials, have very non-random behaviour in the corresponding situation, i.e. $\Phi_p(x)$ never has a root modulo p .

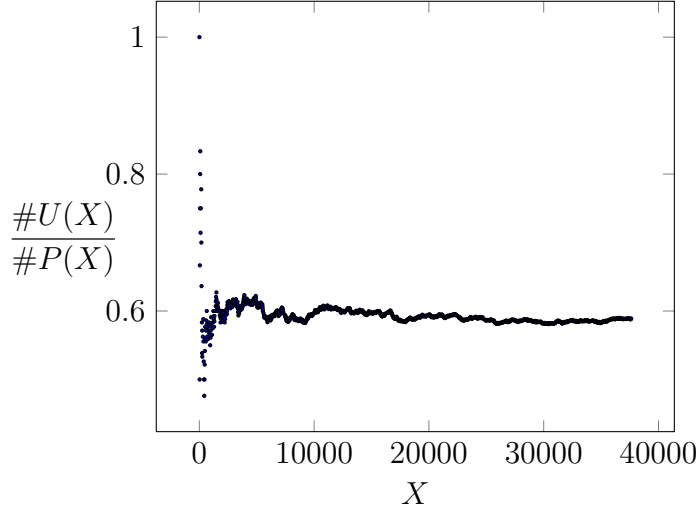


FIGURE 5. Let $T(X) = \{p \leq X : p \text{ prime}, p \equiv 11 \pmod{12}\}$ and $U(X) = \{p \in T(X) : p \in P_{3,c} \text{ for some } c\}$. The plot shows the ratio $\#U/\#T$ for $X \leq 37619$.

However, this raises an interesting general question.

Question 5.2. *As the integer n and prime p vary, what is the splitting behaviour of $\Phi_{n,0}(c)$ modulo p ?*

For a polynomial $f \in \mathbb{Z}[x]$, the splitting behaviour modulo primes is understood via the Tchebotarev Density Theorem. However, cyclotomic polynomials have different statistics than generic polynomials, since their Galois groups are necessarily abelian. To what extent are dynatomic polynomials generic?

6. FIXED n AND VARIABLE c, d

In this section, we investigate $D_{d,c}$ from a different perspective: for a fixed $n \in \mathbb{Z}$, in which $D_{d,c}$ does it appear? Let $H_n = \{(d, c) : n \in D_{d,c}\}$.

Proposition 6.1. *For any integers $d, c \in \mathbb{Z}$, where $d \geq 2$, we have the following.*

- (1) *If $n \mid c$, then $(d, c) \in H_n$.*
- (2) *If $d \equiv 1 \pmod{n-1}$ and n is prime, then $(d, c) \in H_n$.*
- (3) *If $(d, c_0) \in H_n$, then $(d, c) \in H_n$ whenever $c \equiv c_0 \pmod{n}$. Additionally, if d is odd, then $(d, -c) \in H_n$ whenever $(d, c) \in H_n$.*

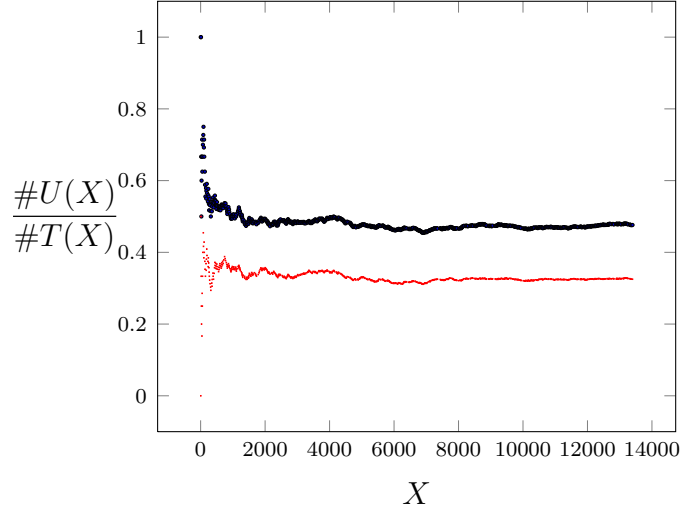


FIGURE 6. Let $T(X) = \{p \leq X : p \text{ prime}, p \equiv 5 \pmod{6}\}$ and $U(X) = \{p \in T(X) : p \in P_{9,c} \text{ for some } c\}$. The plot shows the ratio $\#U/\#T$ for $X \leq 13397$ [upper set]. Of the primes in $U(X)$, roughly two-thirds of them are $11 \pmod{12}$ [lower set].

Proof. The first two properties are immediate from Theorem 1.5. For the third, set $\phi_c(x) = x^d + c$. If $c \equiv c_0 \pmod{n}$, then ϕ_c and ϕ_{c_0} are identical over $\mathbb{Z}/n\mathbb{Z}$. Hence $(d, c) \in H_n$ if and only if $(d, c_0) \in H_n$. Moreover, if d is odd, then $\phi_{-c}(x) = -\phi_c(-x)$. Thus if $\phi_c^n(0) \equiv 0 \pmod{n}$, then $\phi_{-c}^n(0) \equiv 0 \pmod{n}$. \square

Finally, we have a result regarding the powers of d when d is prime.

Theorem 6.2. *If d is prime, there exist d -adic integers a_1, a_2, \dots, a_{d-1} , where $a_1 \equiv 1 \pmod{d}$, $a_2 \equiv 2 \pmod{d}$, \dots , $a_{d-1} \equiv d-1 \pmod{d}$, such that if $c \equiv 0, a_1, a_2, \dots, a_{d-1} \pmod{d^n}$, then $(d, c) \in H_{d^n}$.*

Proof. Let d be prime. From Theorem 1.5, we have $d \in D_{d,c}$ for all $c \in \mathbb{Z}$. In particular, $W_d \equiv 0 \pmod{d}$ for $c \equiv 0, 1, \dots, d-1 \pmod{d}$. Considering W_d as a function in c (e.g. $W_d(c) = (\phi^{d-1}(0))^d + c$), we see that $\frac{d}{dc}W_d(c) \equiv 1 \pmod{d}$. Thus by Hensel's Lemma, each value modulo d lifts to a unique d -adic solution. Namely, if $a_0, a_1, a_2, \dots, a_{d-1} \in \mathbb{Z}_d$ are these lifts (where $a_i \equiv i \pmod{d}$) and $c \equiv a_i \pmod{d^n}$ for one of these a_i , then $W_d(c) \equiv 0 \pmod{d^n}$. It now follows from rigid divisibility that if $d^n \mid W_d$, then $d^n \mid W_{d^n}$. It is straightforward to verify that $a_0 = 0$. \square

REFERENCES

- [1] Shair Ahmad. Cycle structure of automorphisms of finite cyclic groups. *J. Combinatorial Theory*, 6:370–374, 1969.
- [2] Juan José Alba González, Florian Luca, Carl Pomerance, and Igor E. Shparlinski. On numbers n dividing the n th term of a linear recurrence. *Proc. Edinb. Math. Soc. (2)*, 55(2):271–289, 2012.
- [3] Richard André-Jeannin. Divisibility of generalized Fibonacci and Lucas numbers by their subscripts. *Fibonacci Quart.*, 29(4):364–366, 1991.
- [4] A.S. Bang. Talthetheoretiske undersogelser, 1886.
- [5] Robert L. Benedetto, Dragos Ghioca, Benjamin Hutz, Pär Kurlberg, Thomas Scanlon, and Thomas J. Tucker. Periods of rational maps modulo primes. *Math. Ann.*, 355(2):637–660, 2013.
- [6] L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudorandom number generator. *SIAM J. Comput.*, 15(2):364–383, 1986.
- [7] R. D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. (2)*, 15(1-4):30–48, 1913/14.
- [8] Mei-Chu Chang. On periods modulo p in arithmetic dynamics. *C. R. Math. Acad. Sci. Paris*, 353(4):283–285, 2015.
- [9] Kevin Doerksen and Anna Haensch. Primitive prime divisors in zero orbits of polynomials. *Integers*, 12(3):465–472, 2012.
- [10] Avram Gottschlich. On positive integers n dividing the n th term of an elliptic divisibility sequence. *New York J. Math.*, 18:409–420, 2012.
- [11] Spencer Hamblen, Rafe Jones, and Kalyani Madhu. The density of primes in orbits of $z^d + c$. *Int. Math. Res. Not. IMRN*, (7):1924–1958, 2015.
- [12] Verner E. Hoggatt, Jr. and Gerald E. Bergum. Divisibility and congruence relations. *Fibonacci Quart.*, 12:189–195, 1974.
- [13] Patrick Ingram and Joseph H. Silverman. Primitive divisors in arithmetic dynamics. *Math. Proc. Cambridge Philos. Soc.*, 146(2):289–302, 2009.
- [14] Dov Jarden. Divisibility of terms by subscripts in Fibonacci’s sequence and associate sequence. *Rivon Lematematika*, 13:51–56, 1959.
- [15] Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc. (2)*, 78(2):523–544, 2008.
- [16] Rudolf Lidl and Gary L. Mullen. Cycle structure of Dickson permutation polynomials. *Math. J. Okayama Univ.*, 33:1–11, 1991.
- [17] Edouard Lucas. Theorie des Fonctions Numeriques Simplement Periodiques. *Amer. J. Math.*, 1(4):289–321, 1878.
- [18] A. Peinado, F. Montoya, J. Muñoz, and A. J. Yuste. Maximal periods of $x^2 + c$ in \mathbb{F}_q . In *Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001)*, volume 2227 of *Lecture Notes in Comput. Sci.*, pages 219–228. Springer, Berlin, 2001.
- [19] J. M. Pollard. A Monte Carlo method for factorization. *Nordisk Tidskr. Informationsbehandling (BIT)*, 15(3):331–334, 1975.
- [20] Brian Rice. Primitive prime divisors in polynomial arithmetic dynamics. *Integers*, 7:A26, 16, 2007.
- [21] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.
- [22] Joseph H. Silverman. Variation of periods modulo p in arithmetic dynamics. *New York J. Math.*, 14:601–616, 2008.

- [23] Joseph H. Silverman. Primitive divisors, dynamical Zsigmondy sets, and Vojta's conjecture. *J. Number Theory*, 133(9):2948–2963, 2013.
- [24] Joseph H. Silverman and Katherine E. Stange. Terms in elliptic divisibility sequences divisible by their indices. *Acta Arith.*, 146(4):355–378, 2011.
- [25] Chris Smyth. The terms in Lucas sequences divisible by their indices. *J. Integer Seq.*, 13(2):Article 10.2.4, 18, 2010.
- [26] Lawrence Somer. Divisibility of terms in Lucas sequences by their subscripts. In *Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992)*, pages 515–525. Kluwer Acad. Publ., Dordrecht, 1993.
- [27] Lawrence Somer. Divisibility of terms in Lucas sequences of the second kind by their subscripts. In *Applications of Fibonacci numbers, Vol. 6 (Pullman, WA, 1994)*, pages 473–486. Kluwer Acad. Publ., Dordrecht, 1996.
- [28] Troy Vasiga and Jeffrey Shallit. On the iteration of certain quadratic maps over $\text{GF}(p)$. *Discrete Math.*, 277(1-3):219–240, 2004.
- [29] Gary Walsh. On integers n with the property $n \mid f_n$, 1986.
- [30] K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.*, 3(1):265–284, 1892.

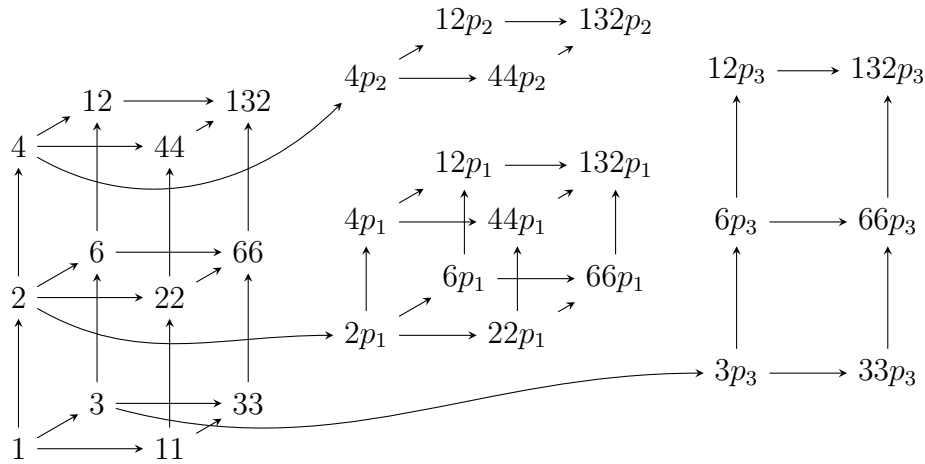


FIGURE 7. A graphical representation of a portion of $D_{3,4}$. Here $p_1 = 17$, $p_2 = 5$, and $p_3 = 26203$. To avoid clutter, not every edge between the vertices shown here is depicted.

BOULDER HIGH SCHOOL, 1604 ARAPAHOE AVE, BOULDER, CO 80302

E-mail address: annieboulder@gmail.com

WESTERN NEW ENGLAND UNIVERSITY, 1215 WILBRAHAM ROAD, SPRINGFIELD, MA
01119

E-mail address: thomas.alden.gassert@gmail.com

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF COLORADO, CAMPUS BOX 395, BOUL-
DER, COLORADO 80309-0395

E-mail address: kstange@math.colorado.edu